GeT a CAKE: Generic Transformations from Key Encaspulation Mechanisms to Password Authenticated Key Exchanges

Hugo Beguinet[12], Céline Chevalier[13], David Pointcheval[1], Thomas Ricosset[2], and Mélissa Rossi[4]

[1] DIENS, École Normale Supérieure, CNRS, Inria, PSL University, Paris, France,
hugo.beguinet, celine.chevalier, david.pointcheval@ens.fr
[2] Thales, Gennevilliers, France,
hugo.beguinet, thomas.ricosset@thalesgroup.com
[3] CRED, Université Paris-Panthéon-Assas, Paris, France
[4] ANSSI, Paris, France,
melissa.rossi@ssi.gouv.fr

Abstract. Password Authenticated Key Exchange (PAKE) have become a key building block in many security products as they provide interesting efficiency/security trade-offs. Indeed, a PAKE allows to dispense with the heavy public key infrastructures and its efficiency and portability make it well suited for applications such as Internet of Things or e-passports. With the emerging quantum threat and the effervescent development of post-quantum public key algorithms in the last five years, one would wonder how to modify existing password authenticated key exchange protocols that currently rely on Diffie-Hellman problems in order to include newly introduced and soon-to-be-standardized post-quantum key encapsulation mechanisms (KEM). A generic solution is desirable for maintaining modularity and adaptability with the many post-quantum KEM that have been introduced.

In this paper, we propose two new generic and natural constructions proven in the Universal Composability (UC) model to transform, in a black-box manner, a KEM into a PAKE with very limited performance overhead: one or two extra symmetric encryptions. Behind the simplicity of the designs, establishing security proofs in the UC model is actually non-trivial and requires some additional properties on the underlying KEM like fuzziness and anonymity. Luckily, post-quantum KEM protocols often enjoy these two extra properties. As a demonstration, we prove that it is possible to apply our transformations to Crystals-Kyber, a lattice-based post-quantum KEM that will soon be standardized by the National Institute of Standards and Technology (NIST).

In a nutshell, this work opens up the possibility to securely include post-quantum cryptography in PAKE-based real-world protocols.

Establishing security proofs in the UC frameworks requires the KEM to have properties like Fuzziness and Anonymity which is apparently enjoyed by the Kyber family.

Then, does it also mean that if a PAKE protocol uses Kyber KEM and the proof is given in the BPR model, it will still be UC secure?

Keywords: Key Encapsulation Mechanism · Password-Authenticated Key Exchange · Universal Composability